UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,096	12/05/2003	Anders M. E. Samuelsson	MS1-1696US	8822

22801 7590 11/14/2008

LEE & HAYES PLLC
601 W Riverside Avenue
Suite 1400
SPOKANE, WA 99201

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
11/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,096	SAMUELSSON ET AL.	
	Examiner	Art Unit	
	BENJAMIN A. KAPLAN	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5, 8-17, and 19 -32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 8-17, and 19 -32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the most recent papers filed on 7/3/2008.

2. Claims 1-5, 8-17 & 19-32 are pending.

3. Claims 1, 14, 22 & 28 are amended.

4. Claims 1-5, 8-17 & 19-32 are rejected.

Response to Arguments and Amendments

5. The rejection of claims 22-27 under 35 USC § 101 is withdrawn.

6. Applicant's arguments with respect to claims 1-5, 8-17 & 19-32 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 3, 4, 8-14 & 19-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Unites States Patent Number US 7,093,292 B1 (Pantuso).

As per Claim 1: Pantuso teaches:

- receiving an event from a first security engine

(Pantuso, Column 4, Lines 21-33, "As shown in FIG. 3, network communications are initially established with a plurality of computers with firewalls over a network. See operation 302. As mentioned earlier, the firewalls are adapted for collecting information relating to intrusion activity. In the context of the present description, intrusion activity may refer to any information that is indicative of or is capable of being used to identify any security-related activity (i.e. an intrusion, virus, hacker activity, security breach, etc.). Once the communication is established, the information is collected from the firewalls of the computers utilizing the network in operation 302. As an option, the information may be transmitted utilizing an HTTP protocol.").

Firewalls submit reports of activity.

- identifying a second security engine configured to utilize information contained in the event

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

The rules are provided to other firewalls.

- wherein the second security engine is unaware of the first security engine

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

- communicating the information contained in the event to the second security engine, wherein the event corresponds to identifying a password that does not comply with predetermined criteria

(Pantuso, Column 1, Lines 34-31, "There are many methods of detecting and protecting against hackers. For example, passwords, heuristic analysis of network activity, etc. may be used for such purpose. Recently, there has been work to generate central databases of hacker-related information that may be used to identify patterns indicative of intrusion activity, and respond accordingly. One example of such databases may found by reference to www.hackerwatch.org.").

As per Claim 3: The rejection of claim 1 is incorporated and further Pantuso teaches:

- the event identifies an action performed by the first security engine in response to a detected vulnerability

(Pantuso, Column 3, Lines 24-30, "The firewalls installed on the data computers 104 or user computers 106 may be equipped with the ability of monitoring intrusion activity. Initially, network communications are established with a plurality of the computers with the firewalls over a network. This may be carried by a central server or the like. In use, the firewalls are adapted for collecting information relating to intrusion activity.").

As per Claim 4: The rejection of claim 1 is incorporated and further Pantuso teaches:

- the first security engine and the second security engine are application programs

(Pantuso, Column 4, Lines 10-14, "A preferred embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, along with an object oriented programming methodology. Object oriented programming (OOP) has become increasingly used to develop complex applications.").

As per Claim 8: The rejection of claim 1 is incorporated and further Pantuso teaches:

- the first security engine is a vulnerability analysis application program

(Pantuso, Column 3, Lines 16-26, "A plurality of the data computers 104 or user computers 106 may be each equipped with a firewall. In one example, the firewalls may each include a software application installed directly on the data computers 104 or user

computers 106 in the form of personal firewalls. Of course, other traditional approaches may also be employed, such as utilizing a separate hardware component between the computer and the network.

The firewalls installed on the data computers 104 or user computers 106 may be equipped with the ability of monitoring intrusion activity.").

As per Claim 9: The rejection of claim 1 is incorporated and further Pantuso teaches:

- identifying a third security engine configured to utilize information contained in the event; and communicating the information contained in the event to the third security engine

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 10: The rejection of claim 1 is incorporated and further Pantuso teaches:

- receiving an updated security policy, identifying at least one security engine associated with the updated security policy; and providing the updated security policy to the identified security engine

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 11: The rejection of claim 1 is incorporated and further Pantuso teaches:

- receiving a request for data from the first security engine; and communicating the requested data to the first security engine

(Pantuso, Column 4, Lines 43-67, "Of course, the firewall-equipped computers may be adapted to manually or automatically send such information in response to the detection of intrusion activity at the computer.

Once the information is collected by the central server, the information is analyzed to ascertain intrusion activity in operation 304. As an option, this may be accomplished heuristically. See operation 304. For example, the information may be analyzed for patterns that are indicative of intrusion activity. For reasons that will soon become apparent, the analysis may also include the identification of a source of the intrusion activity.

By way of example, if it is found that a large number of computers are the subject of the same port scans, this may be assumed to indicate intrusion activity. In another example, if a large number of computers receive an email with the phrase "OPEN

ATTACHMENT" in the subject header, this too may be considered intrusion activity. Of course, any other analysis may be used which is capable of detecting intrusion activity.

Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 12: The rejection of claim 1 is incorporated and further Pantuso teaches:

- storing information contained in the event in a central location accessible to a plurality of security engines

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 13: The rejection of claim 1 is incorporated and further Pantuso teaches:

- one or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 1

See (Pantuso, Figure 2) for a picture of the computer hardware environment.

As per Claim 14: Pantuso teaches:

- receiving a security-related event from a first security-related application program, the security-related event being associated with a system state

(Pantuso, Column 4, Lines 21-33, "As shown in FIG. 3, network communications are initially established with a plurality of computers with firewalls over a network. See operation 302. As mentioned earlier, the firewalls are adapted for collecting information relating to intrusion activity. In the context of the present description, intrusion activity may refer to any information that is indicative of or is capable of being used to identify any security-related activity (i.e. an intrusion, virus, hacker activity, security breach, etc.). Once the communication is established, the information is collected from the firewalls of the computers utilizing the network in operation 302. As an option, the information may be transmitted utilizing an HTTP protocol.").

Firewalls submit reports of activity.

- identifying information contained in the security-related event; identifying a second security-related application program associated with the information contained in the security-related event

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

The rules are provided to other firewalls.

- wherein the second security-related application program is unaware of the first security-related application program

- communicating the information contained in the security-related event to the second security-related application program

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

As per Claim 19: The rejection of claim 14 is incorporated and further Pantuso teaches:

- receiving system state information from a third security-related application program; and storing the system state information such that the system state information is accessible to the first security-related application program and the second security-related application program

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 20: The rejection of claim 14 is incorporated and further Pantuso teaches:

- identifying a third security-related application program associated with the information contained in the security-related event; and communicating the information contained in the security-related event to the third security-related application program

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 21: The rejection of claim 14 is incorporated and further Pantuso teaches:

- one or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 14

See (Pantuso, Figure 2) for a picture of the computer hardware environment.

As per Claim 22: Pantuso teaches:

- One or more tangible computer-readable media having stored thereon a computer program executed by one or more processors, comprising: See (Pantuso, Figure 2) for a picture of the computer hardware environment.

- a first security engine associated with a first type of security attack, the first security engine including configuration to detect a password that does not comply with predetermined criteria

(Pantuso, Column 4, Lines 21-33, "As shown in FIG. 3, network communications are initially established with a plurality of computers with firewalls over a network. See operation 302. As mentioned earlier, the firewalls are adapted for collecting information relating to intrusion activity. In the context of the present description, intrusion activity may refer to any information that is indicative of or is capable of being used to identify any security-related activity (i.e. an intrusion, virus, hacker activity, security breach, etc.). Once the communication is established, the information is collected from the firewalls of the computers utilizing the network in operation 302. As an option, the information may be transmitted utilizing an HTTP protocol.").

(Pantuso, Column 1, Lines 34-31, "There are many methods of detecting and protecting against hackers. For example, passwords, heuristic analysis of network activity, etc. may be used for such purpose. Recently, there has been work to generate central databases of hacker-related information that may be used to identify patterns indicative of intrusion activity, and respond accordingly. One example of such databases may found by reference to www.hackerwatch.org.").

- a second security engine associated with a second type of security attack wherein the second security engine is unaware of the first security engine

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

There are a plurality of firewalls and numerous different attacks that they are set up to deal with.

- an event manager coupled to receive events from the first security engine and the second security engine, the event manager further to identify information contained in the events and to identify at least one security engine associated with information contained in a particular event, and further to communicate the information contained in the particular event to the at least one security engine

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

The central server for the firewalls is the event manager.

As per Claim 23: The rejection of claim 22 is incorporated and further Pantuso teaches:

- the information contained in the events identifies a type of security attack

(Pantuso, Column 4, Lines 21-33, "As shown in FIG. 3, network communications are initially established with a plurality of computers with firewalls over a network. See operation 302. As mentioned earlier, the firewalls are adapted for collecting information relating to intrusion activity. In the context of the present description, intrusion activity may refer to any information that is indicative of or is capable of being used to identify any security-related activity (i.e. an intrusion, virus, hacker activity, security breach, etc.). Once the communication is established, the information is collected from the firewalls of the computers utilizing the network in operation 302. As an option, the information may be transmitted utilizing an HTTP protocol.").

As per Claim 24: The rejection of claim 22 is incorporated and further Pantuso teaches:

- the information contained in each event identifies an action taken in response to a security attack

(Pantuso, Column 3, Lines 24-30, "The firewalls installed on the data computers 104 or user computers 106 may be equipped with the ability of monitoring intrusion activity. Initially, network communications are established with a plurality of the computers with the firewalls over a network. This may be carried by a central server or

the like. In use, the firewalls are adapted for collecting information relating to intrusion activity.").

As per Claim 25: The rejection of claim 22 is incorporated and further Pantuso teaches:

- the information contained in the events includes system state information.

(Pantuso, Column 1, Lines 34-31, "There are many methods of detecting and protecting against hackers. For example, passwords, heuristic analysis of network activity, etc. may be used for such purpose. Recently, there has been work to generate central databases of hacker-related information that may be used to identify patterns indicative of intrusion activity, and respond accordingly. One example of such databases may found by reference to www.hackerwatch.org.").

As per Claim 26: The rejection of claim 22 is incorporated and further Pantuso teaches:

- a third security engine coupled to the event manager and associated with a third type of security attack

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then

received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

There are a plurality of firewalls and numerous different attacks that they are set up to deal with.

As per Claim 27: The rejection of claim 22 is incorporated and further Pantuso teaches:

- a storage device coupled to the event manager, the first security engine and the second security engine, the storage device to store event information

See (Pantuso, Figure 2) for a picture of the computer hardware environment. If the central server didn't store the event information it wouldn't have the information to make its judgments with.

As per Claim 28: Pantuso teaches:

- One or more tangible computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to: See (Pantuso, Figure 2) for a picture of the computer hardware environment.

- receive a first security-related event from a first service, the first security-related event corresponding to a network-related aspect of a system state;

(Pantuso, Column 4, Lines 21-33, "As shown in FIG. 3, network communications are initially established with a plurality of computers with firewalls over a network. See operation 302. As mentioned earlier, the firewalls are adapted for collecting information relating to intrusion activity. In the context of the present description, intrusion activity may refer to any information that is indicative of or is capable of being used to identify any security-related activity (i.e. an intrusion, virus, hacker activity, security breach, etc.). Once the communication is established, the information is collected from the firewalls of the computers utilizing the network in operation 302. As an option, the information may be transmitted utilizing an HTTP protocol.").

Firewalls submit reports of activity.

- identify information contained in the first security-related event

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

- receive a second security-related event from a second service, wherein the second service is unaware of the first service

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to

a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

- identify information contained in the second security-related event

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

- communicate information contained in the first security-related event to the second service; and communicate information contained in the second security-related event to the first service

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

As per Claim 29: The rejection of claim 28 is incorporated and further Pantuso teaches:

- the first security-related event identifies a particular type of security attack

(Pantuso, Column 4, Lines 63-67, "Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 30: The rejection of claim 28 is incorporated and further Pantuso teaches:

- the one or more processors further store the information contained in the first security-related event and the information contained in the second security-related event for access by other services

(Pantuso, Column 4, Lines 47-67, "Once the information is collected by the central server, the information is analyzed to ascertain intrusion activity in operation 304. As an option, this may be accomplished heuristically. See operation 304. For example, the information may be analyzed for patterns that are indicative of intrusion activity. For reasons that will soon become apparent, the analysis may also include the identification of a source of the intrusion activity.

By way of example, if it is found that a large number of computers are the subject of the same port scans, this may be assumed to indicate intrusion activity. In another example, if a large number of computers receive an email with the phrase "OPEN ATTACHMENT" in the subject header, this too may be considered intrusion activity. Of course, any other analysis may be used which is capable of detecting intrusion activity.

Once any intrusion activity is identified (see decision 305), rules may be generated for preventing the intrusion activity utilizing the firewalls. See operation 306. Next, in operation 308, the rules are transmitted to the firewalls of the computers utilizing the network.").

As per Claim 31: The rejection of claim 28 is incorporated and further Pantuso teaches:

- the one or more processors further communicate information contained in the first security-related event to a third service

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

There are a plurality of firewalls subscribed to the central server.

As per Claim 32: The rejection of claim 28 is incorporated and further Pantuso teaches:

- the first service is associated with a first type of security attack and the second service is associated with a second type of security attack

(Pantuso, Column 2, Lines 10-17, "From the perspective of each firewall, information relating to intrusion activity associated with a computer is initially collected. Further, the information is transmitted from the firewall associated with the computer to a central server utilizing the network. A response from the central server is then received utilizing the network. As mentioned before, the firewall is adapted for preventing the intrusion activity utilizing the response.").

There are a plurality of firewalls and numerous different attacks that they are set up to deal with.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2 & 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pantuso in view of United States Patent Number 4,970,504 (Chen).

As per Claim 2: The rejection of claim 1 is incorporated and further Pantuso does not explicitly teach the following limitation:

- the event identifies a password that does not comply with a length criteria

However Chen in analogous art does teach the above limitation:

(Chen, Column 4, Lines 11-15, "If the keyed-in password does not equal the currently stored password, including unequal number and inconsistent length, the CPU 10 will then output a light signal LS to the LED 36 to indicate that the keyed-in password is incorrect (block 122).").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Chen in to the method of Pantuso in order to take advantage of know existing criteria for analysis of alarm worthy conditions.

As per Claim 5: The rejection of claim 1 is incorporated and further Pantuso does not explicitly teach the following limitation:

- the event identifies a password that does not include one or more required characters

However Chen in analogous art does teach the above limitation:

(Chen, Column 4, Lines 11-15, "If the keyed-in password does not equal the currently stored password, including unequal number and inconsistent length, the CPU 10 will then output a light signal LS to the LED 36 to indicate that the keyed-in password is incorrect (block 122).").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Chen in to the method of Pantuso in order to take advantage of know existing criteria for analysis of alarm worthy conditions.

11. Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pantuso in view of United States Patent Application Number US 2003/0204632 A1 (Willebeek-LeMair et al.).

As per Claims 15-17: The rejection of claim 14 is incorporated and further Pantuso does not explicitly teach the following limitations:

- the information includes whether a network connection is wired or wireless

- the information includes whether a host computer is accessing a corporate network

- the information includes whether a host computer is accessing an unknown network

However Willebeek-LeMair et al. in analogous art does teach the above limitation:

(Willebeek-LeMair et al., Paragraph [0081], "Reference is now made to FIG. 6 wherein there is shown a block diagram of a threat prevention appliance 500 that utilizes the unified network defense system 10 of FIGS. 1 and 2. The threat prevention appliance 500 is configured as a network element in the protected network 14. The appliance 500 includes a number of external physical interfaces 502 that allow the appliance to be connected to the outside world (i.e., the untrusted world outside of the protected network 14). As an example, the untrusted world may comprise any one or more of the following: a wide area network (WAN); a virtual private network (VPN) server; local area network (LAN) clients; a wireless or remote access server; and, an

untrusted network (such as the Internet). A number of internal physical interfaces 504 are included to allow the appliance 500 to be connected to the elements of the protected (trusted) network 14. As an example, the elements of the protected network 14 may include: a router; special server types (for example, HTTP, SMTP, FTP, DNA, and the like); an intranet; personal computers; and, network zones. It will be recognized (although not specifically illustrated) that the physical interfaces 502 and 504 may be interconnected with other as desired in configuring the interconnection of the trusted network 14 and the untrusted network.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Willebeek-LeMair et al. in to the method of Pantuso in order to take advantage of know existing criteria for analysis of security alert worthy conditions.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434